УДК 004.8/681.5 DOI: https://doi.org/10.32515/2664-262X.2022.6(37).1.77-87

В.С. Гермак, викл., **Р.М. Минайленко,** доц., канд. техн. наук
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна
e-mail: aron70@ukr.net

Проблема захисту обміну даними між мікропроцесорними пристроями в системах IoT

В статті проведено аналіз методів протидії ботнет в системах IoT. Сьогодні, інтернет речей став популярним терміном для опису сценаріїв, у яких інтернетз'єднання і обчислювальна здатність поширюються на безліч об'єктів, пристроїв, датчиків і т.д.

Основною концепцією IoT є можливість підключення всіляких об'єктів (речей), які людина може використовувати в повсякденному житті. Ці об'єкти (речі) повинні бути оснащені вбудованими датчиками або сенсорами, які мають можливість обробляти інформацію, що надходить з навколишнього середовища, обмінюватися нею і виконувати певні дії в залежності від отриманої інформації.

Відсутність на даний час стандартів для захисту таких автономних мереж дещо сповільнює впровадження інтернету речей у повсякденне життя, тому у швидкозростаючій галузі IOT-технологій, яка застосовується у всьому світі є численна кількість вразливостей. Захист інформації та конфіденційність є однією з пріоритетних складових під час вибору певної системи. Тому без належної впевненості в безпеці і приватності даних користувача система IoT буде неконкурентноспроможною.
користувач, система IoT, ботнет, захист інформації

Постановка проблеми. Термін «Інтернет речей» (IoT) вперше був введений Кевіном Ештоном щоб описати систему, в якій фізичні об'єкти могли бути пов'язані з датчиками і мережею Інтернет. Ештон ввів цей термін, щоб проілюструвати можливості радіочастотної ідентифікації (*RFID*), яка використовується в корпоративних системах поставок, щоб порахувати і відстежити товари без потреби в людському втручанні. Сьогодні, інтернет речей став популярним терміном для опису сценаріїв, у яких інтернет з'єднання і обчислювальна здатність поширюються на безліч об'єктів, пристроїв, датчиків і т.д [1, 2, 3].

Основною концепцією IoT є можливість підключення всіляких об'єктів (речей), які людина може використовувати в повсякденному житті, наприклад, холодильник, кондиціонер, автомобіль, велосипед і навіть взуття. Всі ці об'єкти (речі) повинні бути оснащені вбудованими датчиками або сенсорами, які мають можливість обробляти інформацію, що надходить з навколишнього середовища, обмінюватися нею і виконувати певні дії в залежності від отриманої інформації. Прикладом впровадження такої концепції є система «розумний будинок» або «розумна теплиця». Такі системи аналізують дані навколишнього середовища і в залежності від показників регулюють, наприклад, температуру в всередині приміщення без втручання людини [4 ,5, 6-15].

Відсутність на даний час стандартів для захисту мереж таких автономних систем певною мірою сповільнює впровадження інтернету речей у повсякденне життя. Тому у швидкозростаючій галузі IoT-технологій, яка застосовується у всьому світі є численна кількість вразливостей. Захист інформації та конфіденційність є однією з пріоритетних складових під час вибору системи споживачем. Без належної впевненості в безпеці і приватності даних користувача система IoT буде не конкурентноспроможною [3, 5, 16, 17].

Аналіз останніх досліджень і публікацій. На сьогоднішній день інтернету речей приділяється увага на найвищому рівні, зокрема починаючи з 2009 року у Брюселі при підтримці Єврокомісії проходять конференції Annual Internet of Things, де виступають з доповідями єврокомісари, науковці та керівники провідних IT-компаній. За прогнозами аналітиків у найближчі роки очікується справжній бум інтернету речей. Так, за прогнозами Gartner, до 2022 року кількість підключених до всесвітньої мережі пристроїв становитиме 29 мільярдів, а дохід від продажу обладнання, програмного забезпечення та послуг становитиме 2,9 трлн дол. Деякі інші аналітичні агентства висловлюють ще більш оптимістичні прогнози [17-21].

Для об'єднання повсякденних речей у мережу потрібні декілька технологій:

– для ідентифікації кожного об'єкту потрібна проста та компактна технологія, яка б мала можливість збирати та накопичувати інформацію про певний предмет. Певною мірою це можна забезпечити за допомогою мікросхем RFID (Radio-Frequency IDentification), які здатні без власного джерела струму передавати інформацію пристроям зчитування. Як альтернатива до даної технології для ідентифікації об'єктів можуть використовуватись QR- коди. Для визначення точного місця знаходження речі можна застосувати технологію GPS, яка вже використовується у смартфонах та навігаторах.

– для відслідковування змін стану елемента або оточуючого середовища об'єкти повинні оснащуватися сенсорами.

– для обробки та накопичення даних з сенсорів потрібен вбудований малогабаритний обчислювальний пристрій (наприклад Raspberry Pi, Intel Edison)

– для обміну інформацією між пристроями можуть бути використані технології бездротових мереж (Wi-Fi, Bluetooth, ZigBee, 6LoWPAN).

Інтеграція з Інтернетом має на увазі те, що пристрої будуть використовувати IP-адресу як унікальний ідентифікатор. Проте, через обмежені адресні простори в IPv4 (що дозволяє використовувати 4,3 мільярда унікальних адрес), об'єктам IP доведеться використовувати IPv6, який забезпечує унікальними адресами мережевого рівня не менше 300 млн пристроїв на одного жителя Землі. Об'єктами в IP будуть не тільки пристрої із сенсорними можливостями, а і виконавчі пристрої (наприклад, лампочки або замки, з можливістю керування через Інтернет). Майбутнє інтернету речей буде неможливим без підтримки IPv6, тобто глобальне впровадження IPv6 у найближчі роки буде мати вирішальне значення для успішного розвитку IP в майбутньому.

Для бездротової передачі даних важливу роль в побудові інтернету речей відіграють наступні характеристики [3, 5, 6]:

– ефективність;

– відмовостійкість;

– адаптивність;

– можливість самоорганізації.

В звя′зку з цим потрібно звернути увагу на стандарт *IEEE 802.15.4*, який використовується для керування енергоефективними персональними мережами, і є основою для протоколів ZigBee, WiFi, Bluetoot, 6LoWPAN.

Серед провідних технологій важливу роль у розповсюдженні інтернету речей відіграють рішення PLC – технології побудови мереж передачі даних по лініях електропередач, оскільки у багатьох додатках присутній доступ до електромереж (наприклад, торгові автомати, банкомати, інтелектуальні лічильники, контролери освітлення).

Постановка завдання. «Розумних» пристроїв стає все більше і за прогнозами, до 2022 року їх кількість в кілька разів перевищить населення планети. Однак виробники все ще приділяють недостатньо уваги їх безпеці: немає нагадувань про

необхідність зміни стандартних паролів при першому налаштуванні, немає повідомлень про появу нових версій прошивок, а сам процес оновлення може бути складний для звичайного користувача. Все це робить IoT-пристрої бажаною ціллю для зловмисників. Тому що їх простіше заразити ніж персональний комп'ютер і при цьому вони можуть займати далеко не останнє місце в домашній інфраструктурі: одні керують усім інтернет-трафіком, інші можуть знімати відео, а треті керують іншими пристроями (наприклад, кліматична установка).

Шкідливе ПЗ для «розумних» пристроїв розвивається не тільки кількісно, але і якісно. В арсеналі зловмисників з'являється все більше експлойтів, які використовуються для самопоширення, а заражені пристрої використовуються для крадіжки персональних даних, видобутку крипто валюти і т.д. [9, 10, 21].

Є декілька простих порад, які можуть мінімізувати ризик зараження пристроїв IoT:

– закрити доступ із зовнішньої мережі до пристрою;

– періодичне перезавантаження допоможе позбутися від уже встановлених шкідників (але в більшості випадків ризик повторного зараження залишається);

– регулярна перевірка наявності нових версій прошивки та оновлення пристрою;

– використання складних паролей довжиною не менше 8 символів, що включають в себе букви різного регістра, цифри та спецсимволи;

– зміна заводських паролей після першого запуску пристрою, під час першого налаштування (навіть якщо пристрій про це не просить);

– закрити / заблокувати «зайві» порти, якщо є така можливість. Наприклад, якщо немає необходності підключатись до роутера по Telnet (порт tcp варто відключити, щоб перекрити зловмисникам можливу лазівку).

Дані поради можуть лише частково усунути проблеми та вразливості пристроїв інтернету речей, але це не вирішує проблему загалом, бо принцип розробки інтернету речей залишається, а значить і нові вразливості будуть знайдені зловмисниками. Тому потрібно віднайти можливість вирішення проблеми безпеки IoT пристроїв, що дозволить відрізати легкий шлях їх ураження, що призведе до подорожчання продажі ботнет як послуги [3, 7, 20].

Отримані результати аналізу IoT, основних вразливостей та методів їх використання показали що:

– джерелом загроз для інтернету речей найчастіше є людина або група людей, вмотивована фінансово, політично або ж ідейно;

– вразливості, які використовуються зловмисниками найчастіше – спричинені низкою недоліків на етапі розробки IoT пристроїв;

– за останні декілька років більшість атак на IoT мали на меті інфікувати пристрій для послідуючого створення ботнет;

– з 2016 року при атаках на IoT пристрої більше 20% атак використовують ботнет Mirai та його модифікації;

На даному етапі розвитку технології IoT – не існує міжнародного стандарту розробки пристроїв та систем інтернету речей, тож їх захищеність є не вирішеним питанням кібербезпеки.

Таким чином, необхідно провести аналіз проблеми безпеки IoT і знайти спосіб системно вирішити найбільш поширену та критичну проблему в системах інтернету речей, а саме – ботнет [3, 5, 20, 21].

Виклад основного матеріалу. Традиційні способи боротьби з ботнет, частіше всього, обмежуються виявленням слабкого місця в їх інфраструктурі, для маніпуляції

або блокування. Найпоширеніший спосіб полягає в тому, щоб співпрацювати з провайдером Інтернет-послуг для отримання доступу та вимкнення центрального компонента, результатом чого буде втрата контролю ботнетом-власникиком і він більше не зможе наказувати. Такі дії часто виконуються під час надзвичайної реакції на інцидент, який вже відбувається, наприклад – атака DDoS. Хоча цей набір дій і виявився ефективним (наприклад, припинення роботи сервера C&C на базі IRC забороняє ботам отримувати команди та машини, які вже беруть участь у нападі рано чи пізно перезавантажуються), але він вимагає доступу до ПК і співпраці з відповідними установами [4-9, 21].

Класичні заходи протидії ботнетам мають три напрямки для атаки:

1. Сервер керування (C&C).
2. Ботнет-трафік.
3. Заражені комп'ютери.

Відключення сервера C&C

Найбільш перспективним підходом є видалення бази ботнету, якою є сервер C&C. Вимкнення C&C хоста дозволяє вивести з ладу весь ботнет за один раз. Але це можливо тільки при виконання наступних умов:

1. Ботнет використовує централізовану структуру.
2. Розташування сервера C&C відоме.
3. Провайдер співпрацює.

Якщо не виконано хоча б одна з цих умов, сервер C&C не може бути видалений. Новіші ботнети більше не покладаються на централізовану структуру. Вони використовують функцію однорангової мережі (P2P) або multiproxy структури для приховування свого походження. Таким чином, малоймовірною є можливість знаходження розташування C&C сервера. Якщо використовуються декілька фіксованих серверів – всі вони повинні бути вилучені. Коли відомо про місцезнаходження, провайдер, який надає сервер C&C, теж повинен співпрацювати. Дуже часто ботнети контролюються з кулестійких хостерів, які не реагують на запити про зловживання або переміщують сервер до дочірніх партнерських компаній, поки не спаде тиск на хостинг. Організації, які відстежують атаки в Інтернеті, отримують багато посилань на можливі сервери C&C, але вони не взмозі обробляти, стежити та перевіряти дії проти кожного запиту про C&C окремо.

Виведення серверів C&C з ладу не завжди схоже на видалення кореня ботнету. Так як заражені комп'ютери також можуть містити функціональні можливості для автономного розповсюдження, а також іншу логіку, яка виконується у разі відключення C&C. Це створює додатковий трафік і може спричинити масштабне зараження обчислювальних пристроїв [9, 10, 11-14].

Розмивання зловмисного трафіку

Якщо сервер C & C не може бути вимкнений, іншим варіантом може бути переспрямування зловмисного трафіку на свердловини. Свердловини записують шкідливий трафік, аналізують його, а потім перенаправляють таким чином, що він не може досягти початкової мети призначення. Одним з прикладів використання свердловин є DDoS нуль-маршрутизація. У випадку, якщо спостерігається трафік, що належить до спроби реалізації DDoS, він скидається, а іноді підраховується для подальшого аналізу. Нуль-маршрутизація DDoS на кордонних маршрутизаторах є перспективним підходом для пом'якшення атак DDoS, але тут з'являються проблеми з надійністю ідентифікації трафіку, пов'язаного з атакою, та розчленуванням потоків даних високої пропускної спроможності на ранніх стадіях. Це можливо, як правило, лише на рівні інтернетпровайдера [15, 19].

Очищення заражених систем

Найбільш стійким контрзаходом проти ботнетів є очищення всіх заражених систем та видалення встановлених ботів. Хоч це і впливає на потужність ботнету, та є найбільш складним в управлінні методом протидії. На сьогоднішній день власники або адміністратори несуть відповідальність за те, щоб їхні системи були чисті від інфекцій. Йдеться лише про рекомендації та технічну консультацію. Оскільки більшість користувачів навіть не знають про зараження своєї ЕОМ, не кажучи вже про можливість видалення зловмисного програмного забезпечення, тож глобальне очищення неможливе. Величезні рекламні кампанії про Conficker та кількість ще заражених систем показують, що навіть при інтенсивних попередженнях – чекати від простих користувачів якихось дій для повного очищення не варто.

Стандартна рекомендація щодо захисту систем від ботнет полягає в тому, щоб використовувати брандмауери та сучасне антивірусне програмне забезпечення (AV). Брандмауери є профілактичною функцією, яка в багатьох випадках блокує зовнішні атаки. Зростаюча кількість вразливостей drive-by-exploits, використовує помилки в браузері користувача для зараження системи та мобільність шкідливих даних на ноутбуках або USB-накопичувачах, відкриває цілий ряд нових векторів зараження, які обходять брандмауери. Антивірусне програмне забезпечення – реактивна функція. Перш ніж віно зможе виявляти щонебудь, підписи мають бути доступними, і шкідливі дані повинні бути на цільовому комп'ютері. Якщо підписів не існує, то систему не можна захистити. Тести різних AV-баз показали, що деякі показники виявлення становлять менше ніж 80%. Після зараження системи бот може розповсюджувати та виконувати шкідливі дії, доки AV-підписи не стануть доступні і зможуть бути використані. Часто AV-бази застаріли і регулярно не оновлюються. Крім того, різні боти вимикають AV-сканери або ховаються такими шляхами, які неможливо виявити звичайними сканерами [19-21].

Загалом, глобальна очистка, яка потрібна щоб ефективно відняти владу у ботнетів, виглядає нездійсненною.

У минулому були дискусії, в яких експерти заявили, що припинення роботи серверів C&C стає марним, оскільки вони майже завжди будуть замінені новими, більш захищеними системами. Ця прискорена гонка озброєнь в кінцевому рахунку призведе до складної технології ботнету швидше. Позитивний підхід залишає потенційну цільову зону наодинці з існуючою загрозою, а обмеження методів пом'якшення наслідків для уникнення або блокування поточних атак - це визнання безсилля. Тому потрібно поєднувати класичні методи боротьби з додатковими проактивними стратегіями [5-10].

Проактивні заходи та стратегії

Класичні контрзаходи є дуже хорошими кроками для пом'якшення впливу ботнет, але останні події показують, що вони малоефективні. Новіші ботнети використовують більш складні технології і заперечують використання класичних контрзаходів через складностіі, описані вище. Незважаючи на те, що нові структури, представлені останніми ботнетами, ускладнюють застосування класичних контрзаходів, вони відкриті для більш агресивної контртактики [14, 17].

Дослідження структури ботнет часто є першим кроком для пошуку початкової точки для можливих контрзаходів. Характерною властивістю всіх ботнет є те, що вони повинні дозволяти новим машинам, які працюють на ненадійних платформах, приєднатися до мережі. Це важливий аспект для підходів до контрзаходів: не обмежуватися лише діяльністю ззовні – можна приєднатися до мережі, виконувати дослідження, будучи частиною інфраструктури самостійно, і навіть можна містити ботнет або зруйнувати його зсередини . Крім того, боти поширюються, щоб заразити більше систем і збільшувати мережу. Зразки шкідливого програмного забезпечення,

які важко отримати, можуть бути проаналізовані (напр. за допомогою реверсінжинірінгу), щоб дізнатися про їх внутрішні компоненти. Дізнавшись про функціональні особливості бота, часто можна створити фальшивий бот, який стане частиною ботнета для спостереження або перешкоджання внутрішнім зв'язкам. Ця процедура можлива, тому що вся інформація про початкове завантаження повинна включатись в бінарні файли шкідливого програмного забезпечення і може бути клонована [4, 7, 14].

Наступальні стратегії можна розділити на три різні категорії:

– пом'якшення наслідків;

– маніпулювання;

– експлуатація.

Ступінь можливої відповідної дії залежить частіше всього від топології використовуваної ботнетом. Зокрема, децентралізовані та рухомі топології можуть залишити лише декілька шансів на подібні контрзаходи.

Стратегії для пом'якшення наслідків є нападними технічними засобами, які уповільнюють роботу ботнетів за рахунок витрачання їх ресурсів. Прикладом можуть бути тимчасові спроби DoS на сервери C&C, створення з'єднань з зараженими машинами або блокування зловмисних доменів.

Стратегії маніпулювання використовують командний рівень [2, 8, 20]. Знання про командні протоколи мають важливе значення для маніпулювання та введення команд. Необхідні знання про протоколи включають використання криптографії. Незважаючи на те, що криптографія може повністю заперечувати перевірку обміну даними про ботнети, але приклад дослідження Waledac показує, як цього можна досягти, навіть якщо використовуються криптографічні методи, такі як RSA та AES.

Можливими маніпуляціями можуть бути зміна або видалення команд DDoS або спаму, а також команд для завантаження та виконання програм, що дозволяє віддалене очищення зараженого пристрою.

Менш агресивні варіанти, ніж виконання програм на віддалених комп'ютерах, можуть полягати у вилученні зібраних особистих даних, таких як кредитні картки чи банківські реквізити, заміни їх підробленою інформацією або у команді, яка зупиняє збір таких даних.

Експлуатація – це особлива стратегія, яка використовує помилки, знайдені в ботах. Подібно помилкам в інших продуктах, їх можна використовувати для виконання дій на заражених машинах. Дана стратегія є найпотужнішою, але і ризикованою, оскільки вразливості можуть легко привести до пошкодження або виходу з ладу систем та пристроїв [2, 20].

Не кожна стратегія може бути застосована до певного ботнету. Деякі з них значною мірою залежать від топології ботнету.

Атака на адресний рівень

Обговорюючи стратегії, спрямовані на маршрутизацію та адресний рівень інфраструктури ботнету – важливо зрозуміти, що механізм маршрутизації, який використовується ботнетом, необхідний для адреси хостів або C&C серверів відповідно. Командний рівень, навпаки, працює на поверхні схеми адресації, щоб забезпечити комунікаційну мережу, яка накладається на взаємопов'язані пристрої.

Найпоширеніший спосіб, коли бот звертається до центрального сервера C&C, – це ім'я DNS, яке перенаправляє до IP-адреси – адресація відбувається у два етапи. Кожна фаза становить потенційну відправну точку для втручання [3, 5, 20].

Наприклад, запити DNS зазвичай обробляються локальним DNS-resolver, який, пересилає запит на авторитетний DNS-сервер. Цим локальним resolver'ом керує адміністратор сайту, і його легко запрограмувати, щоб повернути створену відповідь

на конкретні запити. Те саме стосується і маршрутизації IP. Локальні маршрутизатори можуть бути обладнані елементами таблиці маршрутизації для відключення певних адрес або перенаправлення їх на різні вузли (sinkholing - це термін для перенаправлення спроб підключення до спеціального сервера для ідентифікації заражених машин). Як наслідок, обидва кроки приводять до того, що боти в локальній мережі не можуть зв'язатися з оригінальним сервером C&C, і навіть можуть керуватися псевдосервером. Таке втручання, завжди вимагає стратегії «man in the middle". Проте, не завжди необхідно змінювати конфігурацію вбудованих пристроїв. Існують підходи, які демонструють динаміку модифікації відповідного мережевого трафіку.

Сучасні ботнети використовують більш складні схеми адресації, які також працюють як накладна мережа на базі IP-Інтернету.

Прикладами можуть слугувати однорангові мережі. Вони мають свою власну схему адресації з метою збільшення гнучкості та децентралізації. Для проникнення в адресний рівень таких ботнет необхідна стратегічна позиція. Загальний підхід полягає у введенні ретельно відстеженого та керованого вузла, який є ідеальним клоном оригіналу [1, 3, 19,21].

Якщо C&C серверів не можна досягти фізично, вони повинні бути доступними через Інтернет, оскільки ботам потрібно зв'язуватись з ними для отримання команд. Це може бути використано для послаблення ботнету шляхом створення DoS на сервер. Тоді контрольований союзником DDoS зробить сервер недоступним. Крім того, ботнети часто покладаються на технологію, яка є слабкою до конкретних атак.

Наприклад, протокол транспортного рівня TCP. Черга резервного копіювання TCP-сервера C&C може бути заповнена спробами з'єднання, викликати умови відмови в обслуговуванні, перетворюючи зброю ботнету проти нього. Це особливо корисно для більшості бот-серверів на базі HTTP, де встановлюються нові зв'язки для кожного командного запиту. Були оцінені різні комбінації служб і операційних систем та знайдена атака TCP DoS, якою можна легко керувати не задіюючи великі ресурсами. Під час дослідження можна було достовірно зменшити ймовірність встановлення з'єднань із TCP-серверами до менш ніж 5% тільки з однією наступальною EOM. Один хост може тримати чергу резервної копії служби жертви, блокуючи всі подальші спроби з'єднання і тим самим заважаючи ботам отримувати або надслати запити команд. Така операція може бути розроблена таким чином, щоб неможливо було розрізнити спроби з'єднання з тими, які продукуються ботами. В результаті, будь-яка контрдія, що має на меті заблокувати запити, також заблокує всі "законні" боти. Ці випробування показали, що одна EOM може тримати службу TCP і підтримувати з'єднання як можна довше. Така атака призводить до зменшення кількості ботів, здатних зв'язатися з сервером C&C і брати участь у зловмисних діях [5, 15-21].

Ще одна подібна атака – це флуд посилання або мережі, де знаходиться сервер C&C з пакетами, які споживають всю доступну пропускну здатність. Проте, очевидно, така операція потребує більше ресурсів, тому що потрібно відправляти більше пакетів. Атака віддзеркалення може бути використана для підвищення інтенсивності відправленого трафіку, однак, це потребую підключення сторонніх ресурсів та дозволу власників сайтів.

Атака на командний рівень

Напад на командний рівень ботнет вимагає знання протоколу, який використовується. Простим прикладом може бути мережа на базі IRC, де команда видалення наказує ботам вилучати себе з заражених систем. Багато класичних ботів реалізують таку інструкцію [7, 8, 9].Впровадження команди вимагає або керування сервером C&C, або боти повинні бути перенаправлені на інший сервер, виконавши

атаку на адресний рівень, який потім поширює інструкцію з видалення. Інші боти не мають можливості видалення, але пропонують функції оновлення, які можуть бути використані для заміни шкідливого програмного забезпечення на безпечну прошивку або програму, яка сканує та видаляє бот.

У поєднанні з проникненням на рівнень адрес, стають можливими інші підходи: оригінальні команди можна прослуховувати, перехоплювати та модифікувати. Спеціальний протокол дозволяє здійснити такі перевірки, метою яких є унеможливлення таких маніпуляцій. Однак подібні заходи поки в ботнетах не були виявлені

Загалом, для того, щоб насправді проводити атаку для проникнення у ботнет, необхідна комбінація дій як з адресацією, так і з командним рівнем. Переадресація ботів на контрольований сервер або для знешкодження, або для того, щоб наказати їм виконувати самознищення, ймовірно, є одним з найбільш ефективних контрзаходів на рівні інфраструктури [15, 21].

Експлуатація ботнет системи речей

Стратегії, які базуються на експлуатації використовують той факт, що навіть ботнети містять помилки та дефекти програмування, що призводить до вразливостей, які можуть бути використані для отримання контролю над центральним компонентом (наприклад, C&C-сервером) або через пристрої, заражені ботнетом. Такі вразливості можуть варіюватися від неправильної конфігурації до прогалин в безпеці програмного забезпечення, наприклад, перезавантаження буфера, яке можна виконати дистанційно.

Стратегії пом'якшення наслідків та маніпулювання не є агресивною для самих заражених машин. Винятком є команди, які завантажують та виконують програми. Експлуатація помилок є ще більш агресивною, ніж виконання регулярних програм, оскільки експлуатаційний код часто потребує спеціальної адаптації до цільової операційної системи та мови. Фреймворки, такі як metasploit, допомагають розробляти загальний експлуатаційний код, та існує ще більший ризик того, що віддалені системи будуть виведені зладу. Це слід враховувати, особливо в сценаріях, де заражені системи контролюють критичні інфраструктури [3, 7, 10].

Перш ніж використовувати помилки, необхідно знайти заражені системи. Для децентралізованих топологій їх можна перерахувати шляхом підрахунку спроб підключення до введених ботів. У прямих топологіях ця інформація може бути витягнута з даних осідання. Інші варіанти - це використання honeypots, підписів IDS або сканерів, які сканують діапазони мереж, в пошуках заражених пристроїв..

Достовірні вразливості в ботах знаходили і раніше. Багато варіантів Rbot та Sdbot мають однакову кодову базу, яка містить вразливі функції, подібні до них. Потенційним способом знищення ботнетів стане виявлення заражених машин, використання вразливості в боті та ін'єкцій виконавчого коду, вимикаючого шкідливі програми. Вразливий код все ще можна знайти у свіжому шкідливому програмному забезпеченні. Conficker.B використовує MD6 криптографічну хеш-функцію для своїх цифрових підписів. Було встановлено, що алгоритм MD6 містить вразливість буферного розриву та може бути виправлений у випуску оновлення, яке було негайно включено в Conficker.C. Хоча ця специфічна вразливість в Conficker.B не була використана, це показало, що навіть складне шкідливе програмне забезпечення не захищено від критичних прогалин безпеки.

Допомога проактивноїстратегії протидії

Кількість технічно прийнятних стратегій показує, що існує безліч можливостей активно діяти проти ботнетів, перш ніж вони завдадуть шкоди. Хоча це є технічно можливим, на практиці слід враховувати етичні та юридичні проблеми, які виникають у цих стратегіях.

Загальним викликом щодо багатьох наступальних підходів є те, що вони повинні виконуватися максимально приховано. Команди розробників ботнетів можуть протидіяти особливим спробам зменшення наслідків атак. Можливості маніпуляції можуть бути застарілими при невеликих змінах протоколу або використання цифрових підписів. Крім того, помилки, які використовуються зазвичай можна виправити за короткий час. У випадку, якщо ботнет потрібно вимкнути, це потрібно зробити глобально і швидко, щоб не залишати команді, яка контролює ботнет будь-якого часу для проведення контрзаходів [4, 15].

Експерти вважають, що переслідування розробників ботнету навряд чи матиме сильний вплив на глобальну загрозу. Натомість з ботнетами потрібно боротися на технічному рівні. Проактивні заходи повинні бути зроблені спільними зусиллями груп міжнародної безпеки разом з провладними структурами.

Висновки. Інтернет речей може викликати величезні зміни у повсякденному житті, надавши звичайним користувачам абсолютно новий рівень комфорту. Але якщо елементи такої системи не будуть належним чином захищені від несанкціонованого втручання, за допомогою надійного криптографічного алгоритму, замість користі вони принесуть шкоду, надавши кіберзлочинцям лазівку для підриву інформаційної безпеки.

Оскільки пристрої із вбудованими комп'ютерами зберігають дуже багато інформації про свого власника, зокрема можуть знати його точне місцезнаходження, доступ до такої інформації може допомогти зловмисникам вчинити злочин.

Відсутність на даний час стандартів для захисту таких автономних мереж дещо сповільнює впровадження інтернету речей у повсякденне життя, тому у швидкозростаючій галузі IOT-технологій, яка застосовується у всьому світі є численна кількість вразливостей. Захист інформації та конфіденційність є однією з пріоритетних складових під час вибору споживачем системи. Без належної впевненості в безпеці і приватності даних користувача система IoT буде не конкурентноспроможною.

На сьогоднішній день рівень успішності контрзаходів ботнету залежить в основному від організаційних та політичних загальних умов. З огляду на те, що налагодження співпраці або дипломатичних угод вимагає часу, можна прийти до висновку, що встановлення відповідних відносин, що легітимує співпрацю для спільних дій, не підходить як спеціальна схема боротьби з поточними нападами [7-10].

Ситуація посилюється, враховуючи, що сучасні інфраструктури ботнету не підпадають під відповідальність одного суб'єкта. Натомість, розподілені однорангові мережі працюють у всьому світі, тому вимикання локальних частин (часто не більше, ніж одиничні ЕОМ) не буде ефективним рішенням. В цілому, контрзаходи, які потребують тісної співпраці, сьогодні, як правило, є нездійсненними як з технічних, так і з політичних причин.

Список літератури

1. Check Point Software Tech. LTD . Most Wanted Malware: Attacks Targeting IoT and Networking doubled since, May 2018. URL: https://blog.checkpoint.com/2018/08/15/julys-most-wanted-malware-attacks-targeting-iot-and-networking-doubled-since-may-2018/
2. Menachem Domb . An Adaptive Lightweight Security Framework Suited for IoT. URL: https://www.intechopen.com/books/internet-of-things-technology-applications-and-standardization/an-adaptive-lightweight-security-framework-suited- for-iot
3. Felix LEDER, Tillmann WERNER, and Peter MARTINI. Institute of Computer Science IV, University of Bonn, Germany . Proactive Botnet Countermeas- ures – An Offensive Approaches. URL: http://four.cs.uni-bonn.de/fileadmin/user_upload/leder/proactivebotnetcountermeasures.pdf
4. Ivo van der Elzen Jeroen van Heugten . Techniques for detecting compro- mised IoT devices. URL: http://www.delaat.net/rp/2016-2017/p59/report.pdf

5. Manos Antonakakis . Understanding the Mirai Botnet.
6. Rohan Doshi, Noah Apthorpe, Nick Feamster . Machine Learning DDoS Detection for Consumer Internet of Things Devices.
7. Sebastian-Dan Naste . A multidisciplinary study on DDoS attacks in the EU IoT ecosystem.
8. OWASP–«IoT Vulnerabilities Project» URL: https://www.owasp.rg/index.php/ OWASP_Internet_of_Things_Project#tab=IoT_Vu lnerabilities (hast accessed: 22.10.2019).
9. OWASP IoT. Attack Surface Project. URL: https://www.owasp.org/ index.php/OWASP_Internet_of_Things_Project#tab=IoT_Att ack_Surface_Areas (hast accessed: 22.10.2019)
10. Daniel Elizalde .IoT Hardware – Introduction and Explanation. URL: https://www.iotforall.com/iot-hardware-introduction-explanation/ (hast accessed: 22.10.2019)
11. Earlence Fernandes et al. FlowFence: Practical Data Protection for Emerging IoT Application Frameworks. URL: https://www.usenix.org/ system/files/conference/usenixsecurity16/sec16 _paper_ferna ndes.pdf (hast accessed: 22.10.2019)
12. HESSELDAHL A. The Hacker's Eye View of the Internet of Things. URL: http://recode.net/2015/04/07/a- hackers- eye- view- of- the- internet- of- things/ (hast accessed: 22.10.2019)
13. FERNANDES, E., JUNG, J., AND PRAKASH, A. Security analysis of emerging smart home applications. Ha IEEE Symposium on Security and Privacy (S&P)
14. Yi home camera. URL: https://www. yitechnology.com/yi- home- camera (hast accessed: 22.10.2019).
15. Hewlett Packard Enterprise . Internet of things research study. URL: http:// h20195.www2.hpe.com/V4/getpdf.aspx/4aa5- 4759enw (hast accessed: 22.10.2019).
16. Internet of things (iot) security and privacy recommendations.
17. S. Hilton . Dyn analysis summary of friday october 21 attack. URL: https://dyn.com/blog/ dyn-analysis-summary-of-friday-october- 21- attack/ (hast accessed: 22.10.2019)
18. V.Chandola, A.Banerjee, V.Kumar . Anomaly detection: A survey.*Technikal Report*. 2007 . Vol. 41. p.3
19. E. Eskin, W. Lee, and W. Stolfo . Modeling system call for intrusion detection using dynamic window sizes.
20. Qin, M. and Hwang, K. 2004. Frequent episode rules for internet anomaly detection. In Proceedings of the 3rd IEEE International Symposium on Network Computing and Applications. IEEE Computer Society.
21. M. Miettinen, S. Marchal, I. Hafeez, N. Asokan, A. Sadeghi, S. Tarkoma . Iot sentinel: Automated device-type identification for security enforcement in IoT. Computer Science. 2017. IEEE 37th International Conference on Distributed Computing Systems (ICDCS).

References

1. Check Point Software Tech. LTD . Most Wanted Malware: Attacks Targeting IoT and Networking doubled since, May 2018. URL: https://blog.checkpoint.com/2018/08/15/julys-most-wanted-malware-attacks-targeting-iot-and-networking-doubled-since-may-2018/ [in English].
2. Menachem Domb . An Adaptive Lightweight Security Framework Suited for IoT. URL: https://www.intechopen.com/books/internet-of-things-technology-applications-and-standardization/an-adaptive-lightweight-security-framework-suited- for-iot [in English].
3. Felix LEDER, Tillmann WERNER, and Peter MARTINI. Institute of Computer Science IV, University of Bonn, Germany . Proactive Botnet Countermeas- ures – An Offensive Approaches. URL: http://four.cs.uni-bonn.de/fileadmin/user_upload/leder/proactivebotnetcountermeasures.pdf [in English].
4. Ivo van der Elzen Jeroen van Heugten . Techniques for detecting compro- mised IoT devices. URL: http://www.delaat.net/rp/2016-2017/p59/report.pdf [in English].
5. Manos Antonakakis . Understanding the Mirai Botnet [in English].
6. Rohan Doshi, Noah Apthorpe, Nick Feamster . Machine Learning DDoS Detection for Consumer Internet of Things Devices [in English].
7. Sebastian-Dan Naste . A multidisciplinary study on DDoS attacks in the EU IoT ecosystem. [in English].
8. OWASP–«IoT Vulnerabilities Project» URL: https://www.owasp.rg/index.php/ OWASP_Internet_of_Things_Project#tab=IoT_Vu lnerabilities [in English].
9. OWASP IoT. Attack Surface Project. URL: https://www.owasp.org/ index.php/OWASP_Internet_of_Things_Project#tab=IoT_Att ack_Surface_Areas[in English].
10. Daniel Elizalde .IoT Hardware – Introduction and Explanation. URL: https://www.iotforall.com/iot-hardware-introduction-explanation/ [in English].
11. Earlence Fernandes et al. FlowFence: Practical Data Protection for Emerging IoT Application Frameworks. URL: https://www.usenix.org/ system/files/conference/usenixsecurity16/sec16 _paper_ferna

ndes.pdf [in English].
12. HESSELDAHL A. The Hacker's Eye View of the Internet of Things. URL: http://recode.net/2015/04/07/a- hackers- eye- view- of- the- internet- of- things/ [in English].
13. FERNANDES, E., JUNG, J., AND PRAKASH, A. Security analysis of emerging smart home applications. Ha IEEE Symposium on Security and Privacy (S&P) [in English].
14. Yi home camera. URL: https://www. yitechnology.com/yi- home- camera [in English].
15. Hewlett Packard Enterprise . Internet of things research study. URL: http:// h20195.www2.hpe.com/V4/getpdf.aspx/4aa5- 4759enw [in English].
16. Internet of things (IoT) security and privacy recommendations. Broadband Internet Technical Advisory Group, Inc. 2016. All rights reserved. [in English].
17. S. Hilton . Dyn analysis summary of friday october 21 attack. (2017). URL: https://dyn.com/blog/ dyn-analysis-summary-of-friday-october- 21- attack/[in English].
18. Chandola, V., Banerjee, A. & Kumar, V. (2007). Anomaly detection: A survey. *Technikal Report*. Vol. 41. p.3
19. Eskin, E., Lee, W. & Stolfo, W. (2005). Modeling system call for intrusion detection using dynamic window sizes. *International Conference on Networking* [in English].
20. Qin, M. & Hwang, K. (2004). Frequent episode rules for internet anomaly detection. In Proceedings of the 3rd IEEE International Symposium on Network Computing and Applications. *IEEE Computer Society* [in English].
21. Miettinen, M., Marchal, S., Hafeez, I., Asokan, N., Sadeghi, A. & Tarkoma, S. (2017). Iot sentinel: Automated device-type identification for security enforcement in IoT. *Computer Science. IEEE 37th International Conference on Distributed Computing Systems* (ICDCS) [in English].

Viktoria Germak, lecturer, **Roman Minailenko,** Assoc. Prof., PhD tech. sci.
Kropyvnytskyi, Ukraine

Analysis of Botnet Countermeasures in IoT Systems

The article analyzes the methods of countering botnets in IoT systems. Today, the Internet of Things has become a popular term to describe scenarios in which Internet connectivity and computing power are spread across a multitude of objects, devices, sensors, etc.

The main concept of IoT is the ability to connect all kinds of objects (things) that a person can use in everyday life. These objects (things) must be equipped with built-in sensors or sensors that have the ability to process information coming from the environment, exchange it and perform certain actions depending on the received information.

The current lack of standards for the protection of such autonomous networks somewhat slows down the introduction of the Internet of Things into everyday life, so there are numerous vulnerabilities in the rapidly growing field of IoT technologies, which are used all over the world. Information protection and confidentiality is one of the priority components when choosing a certain system. Therefore, without adequate confidence in the security and privacy of user data, the IoT system will be uncompetitive.

The Internet of Things can cause huge changes in everyday life, bringing a whole new level of comfort to ordinary users. But if the elements of such a system are not properly protected from unauthorized intervention, with the help of a reliable cryptographic algorithm, they will bring harm instead of good, giving cybercriminals a loophole to undermine information security.

Since devices with built-in computers store a lot of information about their owner, including the ability to know their exact location, access to such information can help criminals commit a crime.

To date, the level of success of botnet countermeasures depends mainly on organizational and political general conditions. Given that the establishment of cooperation or diplomatic agreements takes time, it can be concluded that the establishment of appropriate relations that legitimize cooperation for joint action is not suitable as an ad hoc scheme to combat current attacks.

The situation is aggravated, given that modern botnet infrastructures are not under the responsibility of a single entity. In contrast, distributed peer-to-peer networks operate worldwide, so shutting down local parts (often no more than single computers) is not an effective solution. In general, countermeasures that require close cooperation are generally unfeasible today for both technical and political reasons

Experts believe that prosecuting botnet developers is unlikely to have a strong impact on the global threat. Instead, botnets need to be fought on a technical level. Proactive measures should be taken by joint efforts of international security groups together with pro-government structures.

user, IoT system, botnet, information protection

Одержано (Received) 07.09.2022 *Прорецензовано (Reviewed) 29.09.2022*
Прийнято до друку (Approved) 26.09.2022